Question: 1	
What determines how a Symantec Data Center Security: Server Advanced a	agent performs protection?
A. zero-day protection standards	
B. business critical mission controls	
C. prevention and detection policies	
D. industry and governmental regulations	
	Answer: C
Question: 2	
How does Symantec Data Center Security: Server Advanced limit the poten enterprise resources?	tial for exploitation of
A. by ensuring all patches are implemented	
B. by detecting and repairing known malware	
C. by implementing least privilege access controls	
D. by recognizing aggressive software and user behavior	
	Answer: C
Question: 3	
Which feature can be configured using a detection policy?	
A. Closing network back doors by defining ports to be monitored B. De-escalation of Administrator Privileges	
C. Real-Time File Integrity Monitoring	
D. Restricting Access to Externally Connected Devices	
	Answer: C
Question: 4	

Which two statements accurately describe an advantage of using Symantec Data Center Security: Server Advanced prevention policies over traditional malware protection products? (Select two.)

- A. Symantec Data Center Security: Server Advanced prevention policies are proactive in protecting against Malware.
- B. Symantec Data Center Security: Server Advanced prevention policies require infrequent signature updates.
- C. Symantec Data Center Security: Server Advanced prevention policies can be applied to a machine without installing agent software on the host machine.

D. Symantec Data Center Security: Server Advanced prevention policies prote the behavior of all processes running on that system.	, , ,
E. Symantec Data Center Security: Server Advanced prevention policies are p	naπorm agnostic.
- -	Answer: A, D
Question: 5	
Which action applies to prevention policies rather than detection policies?	
 A. they detect changes to files using Real-Time File Integrity Monitoring B. they audit changes to registry keys, files and folders C. they monitor for local events that trigger actions when matched D. they sandbox processes proactively when executed 	
- -	Answer: D
Question: 6	
Which feature can be configured using a detection policy?	
 A. Closing network back doors by defining ports to be monitored B. De-escalation of Administrator Privileges C. Real-Time File Integrity Monitoring D. Restricting Access to Externally Connected Devices 	
	Answer: C
Question: 7	
Which action can the administrator perform using the management console	?
A. Two factor authenticationB. User generated reportsC. Administrator password complexityD. Network bandwidth throttling	
- -	Answer: B
Question: 8	
Which two statements accurately describe Symantec Data Center Security: S failover? (Select two.)	erver Advanced simple

A. The management console uses the first server in the ordered list of management servers when it

sta	rts	u	р

- B. Enables deployment of a set of front-end Tomcat servers without reconfiguring the IT infrastructure
- C. Can provide static load balancing via manual assignment of agents to each Tomcat server
- D. The Symantec Data Center Security: Server Advanced Security Virtual Appliance supports simple failover
- E. An ordered list of management servers for simple failover is maintained by the SQL Data Store

	Answer: B, C
Question: 9	
Which component is excluded from the Symantec Data Center Securi	ty: Server Advanced architecture?
A. Security Virtual Appliance B. Management Server C. IIS Web Server D. Management Console	
	Answer: C
Question: 10	
Which key component stores the policies, agent information, and rea	al-time actionable events?
A. Management ServerB. Database ServerC. Management ConsoleD. Security Virtual Appliance	
	Answer: B